

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of

Communications Assistance for Law
Enforcement Act

RECEIVED

FEB 07 2000

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

CC Docket No. 97-213

BELLSOUTH OPPOSITION

BELLSOUTH CORPORATION

M. Robert Sutherland
Angela N. Brown
1155 Peachtree Street, N.E.
Suite 1700
Atlanta, GA 30309-3610
(404) 249-3392

**BELLSOUTH
TELECOMMUNICATIONS, INC.**

J. Lloyd Nault, II
4300 BellSouth Center
675 West Peachtree Street, N. E.
Atlanta, GA 30375
(404) 335-0737

BELLSOUTH CELLULAR CORP.

S. Kendall Butterworth
1100 Peachtree St., N.E.
Suite 910
Atlanta, GA 30309-4599
(404) 249-0919

BELLSOUTH WIRELESS DATA, L.P.

Michael W. White
10 Woodbridge Center Drive, 4th Floor
Woodbridge, NJ 07095-1106
(732) 602-5453

Date: February 7, 2000

0 + 9
Opposition of BellSouth Corp.
CC Docket No. 97-213
February 7, 2000
Doc No. 118335

TABLE OF CONTENTS

SUMMARY	ii
INTRODUCTION	2
I. THE COMMISSION APPROPRIATELY DETERMINED THAT ONLY A LIMITED SET OF RULES WAS NECESSARY TO ENSURE THAT CARRIERS COMPLY WITH THE SYSTEMS SECURITY AND INTEGRITY PROVISIONS OF CALEA.....	3
II. THE COMMISSION SHOULD REJECT THE DOJ/FBI REQUESTS TO PROMULGATE ADDITIONAL SYSTEMS SECURITY AND INTEGRITY RULES.....	5
A. The Commission Should Deny The DOJ/FBI Proposal To Require Carriers To Maintain A List of Designated Employees.....	7
B. The Commission Should Deny The DOJ/FBI Request To Obtain Personal Information On Designated Employees In Order To Facilitate Background Checks	9
C. The Commission Should Reject The DOJ/FBI Request To Require Designated Employees To Sign Non-Disclosure Agreements	11
D. The Commission Should Affirm Its Denial Of The DOJ/FBI Request To Require Carriers To Provide A Surveillance Status Message	13
E. The Commission Should Not Modify Its Rule Regarding Reporting Suspected System Security Breaches.....	15
CONCLUSION.....	16

SUMMARY

The record developed in this proceeding convincingly demonstrates that the Commission should deny the Petition for Reconsideration filed by the Department of Justice/Federal Bureau of Investigation ("DOJ/FBI Petition") on October 25, 1999. That Petition challenges two of the Commission's orders adopting rules to implement the systems security and integrity provisions of the Communications Assistance for Law Enforcement Act ("CALEA").

Properly refusing to "micro-manage" the corporate policies of carriers, the Commission determined that a focused and limited set of rules was necessary to ensure that carriers satisfy their obligations under CALEA. No additional regulation is warranted. A reasonable set of guidelines – rather than the proposals set forth by the DOJ/FBI – will allow carriers of all sizes the flexibility to tailor their policies and procedures to their individual operations and circumstances. Moreover, the existing statutory and regulatory requirements, the existing policies and procedures of carriers, and the lack of substantial evidence of security breaches all support a finding that no additional rules or modifications are warranted. Accordingly, BellSouth urges the Commission to deny the DOJ/FBI Petition.

Specifically, the Commission should take the following actions:

- (1) deny the DOJ/FBI recommendation that the Commission require carriers to maintain a list of employees designated to facilitate electronic surveillance;
- (2) reject the DOJ/FBI request to obtain personal information on designated employees (including the names, dates of birth, social security numbers, and workplace telephone numbers of these employees);
- (3) deny the DOJ/FBI request that carriers require designated employees to sign non-disclosure agreements and agree to submit to background checks conducted by law enforcement;

- (4) affirm its ruling that CALEA does not require carriers to provide a surveillance status message; and
- (5) reject the DOJ/FBI proposal to require carriers to report breaches "as soon after discovery as is reasonable in light of privacy and safety concerns and the needs of law enforcement."

As demonstrated herein, the Commission has adopted sufficiently detailed requirements obligating carriers to establish policies and procedures to ensure compliance with the systems security and integrity provisions of CALEA. No further regulations or modifications to existing rules are needed.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of

Communications Assistance for Law
Enforcement Act

CC Docket No. 97-213

BELLSOUTH OPPOSITION

BellSouth Corporation, BellSouth Telecommunications, Inc., BellSouth Cellular Corp., and BellSouth Wireless Data, L.P. (collectively "BellSouth")¹ respectfully submit their opposition to the Department of Justice/Federal Bureau of Investigation Petition for Reconsideration ("DOJ/FBI Petition") of the Commission's *Report and Order*² and *Third Report and Order*³ in the above-captioned proceeding.⁴

¹ BellSouth Corporation is a publicly-traded Georgia corporation that holds the stock of BellSouth Enterprises, Inc. ("BSE") and BellSouth Telecommunications, Inc., a Bell operating company providing wireline telephone exchange and exchange access service in parts of Alabama, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, South Carolina and Tennessee ("BST"). BSE holds the stock of BellSouth Cellular Corporation ("BCC"), a Georgia corporation that provides commercial mobile radio service in markets throughout the United States, and holds personal communications service ("PCS") licenses in North Carolina, South Carolina, Georgia and Tennessee. BSC holds a controlling interest in BellSouth Wireless Data, L.P. ("BWD"), a Delaware limited partnership that operates a nationwide, packet-switched wireless data communications network using frequencies licensed by the FCC in the Specialized Mobile Radio ("SMR") Service bandwidth.

² *Communications Assistance for Law Enforcement Act*, Report and Order, FCC 99-11, CC Docket No. 97-213 (rel. March 15, 1999) ("*Report and Order*"), modified by *Communications Assistance for Law Enforcement Act*, Order on Reconsideration, FCC 99-184, CC Docket No. 97-213 (rel. August 2, 1999) ("*Reconsideration Order*").

³ *Communications Assistance for Law Enforcement Act*, Third Report and Order, FCC 99-230, CC Docket No. 97-213 (rel. August 31, 1999) ("*Third Report and Order*").

⁴ Petition for Reconsideration of Section 105 Report and Order, U.S. Department of Justice/Federal Bureau of Investigation, *Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213 (filed Oct. 25, 1999) ("DOJ/FBI Petition").

INTRODUCTION

In 1999, the Commission issued a series of orders adopting rules to implement various provisions of the Communications Assistance for Law Enforcement Act ("CALEA").⁵ This pleading will focus on two of those orders: (1) the *Report and Order*, released on March 15, 1999, in which the FCC established the systems security and integrity regulations that carriers must follow to comply with section 105⁶ of CALEA and section 229⁷ of the Communications Act; and (2) the *Third Report and Order*, released on August 31, 1999, in which the Commission adopted technical requirements for wireline, cellular, and broadband personal communications services ("PCS") carriers to comply with CALEA's assistance capability requirements.

The DOJ/FBI seek reconsideration of a number of Commission rulings in both the *Report and Order* and *Third Report and Order*. Specifically, the DOJ/FBI request that the Commission amend its rules to:

- (1) require carriers to maintain a list of employees designated to facilitate electronic surveillance;⁸
- (2) require the list of designated employees to include the names, dates of birth, social security numbers, and workplace telephone numbers of the designated employees;⁹

⁵ See, e.g., *Report and Order and Reconsideration Order supra* note 2; *Communications Assistance for Law Enforcement Act, Second Report and Order*, FCC 99-229, CC Docket No. 97-213 (rel. August 31, 1999) ("*Second Report and Order*"); *Third Report and Order supra* note 3.

⁶ Section 105 provides as follows: "[a] telecommunications carrier shall ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission." 47 U.S.C. § 1004.

⁷ Section 229 mandates that the Commission prescribe rules to implement the systems security and integrity provisions of CALEA. 47 U.S.C. § 229.

⁸ DOJ/FBI Petition at 5, 6-7.

⁹ *Id.* at 7.

- (3) direct carriers to require designated employees to sign non-disclosure agreements and agree to submit to background checks conducted by law enforcement;¹⁰
- (4) require carriers to generate a "surveillance status message" that would enable law enforcement agencies to verify that unauthorized electronic surveillance is not occurring;¹¹ and
- (5) modify the language of the Commission's rules to require carriers to report breaches "as soon after discovery as is reasonable in light of privacy and safety concerns and the needs of law enforcement."¹²

The Commission should reject all of these requests as unnecessary and burdensome. The agency has already adopted sufficiently detailed requirements obligating carriers to establish policies and procedures that comply with section 105 of CALEA and section 229 of the Communications Act. The DOJ/FBI Petition fails to demonstrate why the Commission should amend or create additional rules implementing these provisions. BellSouth believes that existing carrier policies and procedures, combined with the existing statutory and regulatory prescriptions, provide adequate incentive to ensure that only lawfully authorized electronic surveillance occurs. Accordingly, the Commission should deny the DOJ/FBI Petition.

I. THE COMMISSION APPROPRIATELY DETERMINED THAT ONLY A LIMITED SET OF RULES WAS NECESSARY TO ENSURE THAT CARRIERS COMPLY WITH THE SYSTEMS SECURITY AND INTEGRITY PROVISIONS OF CALEA.

The additional detailed regulation sought by the DOJ/FBI is simply unwarranted. The existing rules are more than adequate to ensure that carriers have policies and procedures in place to conduct lawfully authorized intercepts. In its *Report and Order*, the Commission

¹⁰ *Id.*

¹¹ *Id.* at 8-9.

¹² *Id.* at 10.

appropriately declined “to adopt specific or detailed policies and procedures that telecommunications carriers must include within their internal operating practices”¹³ The Commission instead found it appropriate “to implement a *very limited set of rules* to assist telecommunications carriers in complying with their obligations under section 105 of CALEA and sections 229(b) and (c) of the Communications Act.”¹⁴ In adopting this limited set of rules, the Commission concluded that it was “not the [agency’s] responsibility to ‘micro-manage’ telecommunications carriers’ corporate policies.”¹⁵ Given the persuasive evidence in the record, the Commission elected to “replace much of [its] proposed regulatory scheme with a *minimum set of requirements* intended to allow carriers to develop their own policies and procedures that assure the maintenance of their systems security and integrity in compliance with” the law.¹⁶

The Commission was correct to adopt a focused and limited set of rules. This approach recognizes that a carrier is in the best position to determine how to implement the CALEA systems security and integrity provisions most effectively and efficiently. A minimal set of guidelines allows carriers the flexibility to tailor their policies and procedures to their individual operations and circumstances. By contrast, the increased regulation proposed by the DOJ/FBI will overburden carriers and infringe on the privacy rights of carrier personnel without providing any significantly increased surveillance effectiveness.

The Commission can alleviate any additional hardships on carriers, including small and rural companies, by refusing to require the additional obligations requested by the DOJ/FBI. The

¹³ *Report and Order*, ¶ 18.

¹⁴ *Id.*, ¶ 17 (emphasis added).

¹⁵ *Id.*, ¶ 18.

¹⁶ *Id.*, ¶ 20 (emphasis added).

National Telephone Cooperative Association ("NTCA") has asked the Commission to exempt small, rural telephone companies from the statutory and regulatory obligation¹⁷ to file their systems security and integrity policies and procedures with the Commission.¹⁸ According to the NTCA, an exemption would reduce the burdens placed on small companies.¹⁹ The fact that NTCA is requesting an exemption demonstrates the continued need for flexible Commission security rules.

BellSouth believes that granting the DOJ/FBI proposals will handicap all carriers, not just small ones, by requiring these companies to comply with unnecessary and onerous rules. By contrast, the flexible regulatory framework that the Commission established in its *Report and Order* will enable all carriers, including small and rural companies, to develop policies and procedures that are uniquely tailored to their size and resources. There is already an existing duty under the law requiring *all* common carriers to submit their systems security policies and procedures to the Commission.²⁰ To eliminate any additional burden on carriers, the Commission should deny the DOJ/FBI Petition.

II. THE COMMISSION SHOULD REJECT THE DOJ/FBI REQUESTS TO PROMULGATE ADDITIONAL SYSTEMS SECURITY AND INTEGRITY RULES.

There is no need to impose additional burdens on carriers by adopting the DOJ/FBI proposals. The Commission considered many of the issues raised in the Petition and

¹⁷ See 47 U.S.C. § 229(b)(3); 47 C.F.R. § 64.2105.

¹⁸ Petition for Reconsideration and/or Clarification, National Telephone Cooperative Association, *Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, at 3 (filed Oct. 25, 1999) ("NTCA Petition").

¹⁹ *NTCA Petition at 3.*

²⁰ See *supra* note 17.

appropriately concluded that adopting general rules would be more effective than prescribing detailed requirements to implement the systems security and integrity provisions of CALEA. According to the Commission, its systems security and integrity rules were intended “to provide telecommunications carriers with *guidance for the minimum requirements* necessary to achieve compliance with section 105 of CALEA and sections 229(b) and (c) of the Communications Act *in the least burdensome manner possible.*”²¹

As the record clearly demonstrates and the Commission correctly recognized, many carriers, including BellSouth, already “have existing policies and procedures in place to secure and protect their telecommunications systems in a manner that would comply with section 105 of CALEA.”²² Moreover, the record further demonstrates that telephone companies have a long history of cooperation with law enforcement agencies to facilitate electronic surveillance pursuant to lawful authorization. Contrary to the DOJ/FBI suggestion, the Commission need not give law enforcement “oversight” responsibility for a carrier’s employees.²³ Carriers are thoroughly equipped to manage their own employees while meeting the needs of law enforcement. Furthermore, the DOJ/FBI have failed to provide any substantial evidence of employees committing breaches sufficient to warrant the onerous requirements proposed by law enforcement.

BellSouth urges the Commission to prevent the DOJ/FBI from recalibrating the equilibrium sought by Congress in balancing several important interests. As the legislative history indicates, CALEA was designed to achieve a balance of three important policy

²¹ *Report and Order*, ¶ 18 (emphasis added).

²² *Id.*, ¶ 18.

²³ *See* DOJ/FBI Petition at 3.

objectives: “(1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies.”²⁴ The Commission should not allow law enforcement to tilt the balance inherent in CALEA in its favor by diminishing the equally important goals of privacy and technological advancements.

In addition, the Commission should not give any deference to the DOJ/FBI claim that there exists an “impressive degree of consensus between law enforcement and carriers that these measures are necessary.”²⁵ There is not now – nor has there ever been – a consensus that extensive regulation was necessary to meet the systems security and integrity requirements of CALEA. Obviously, the Commission agreed. After thoroughly reviewing the record and carefully scrutinizing the issues, the Commission correctly found that a minimum set of requirements was sufficient to ensure that carriers have policies and procedures in place to assist law enforcement in conducting authorized electronic surveillance. Accordingly, as discussed more fully below, the Commission should reject the DOJ/FBI requests set forth in the Petition.

A. The Commission Should Deny The DOJ/FBI Proposal To Require Carriers To Maintain A List of Designated Employees.

The Commission should deny (for the second time) the DOJ/FBI recommendation that carriers be required to provide a list of designated employees authorized to conduct lawful

²⁴ H.R. Rep. No. 103-827, at 13 (1994) *reprinted in* 1994 U.S.C.C.A.N 3489 (“House Report”).

²⁵ DOJ/FBI Petition at 5.

surveillance. The DOJ/FBI assert that their new proposal is less restrictive than the former request. Rather than requiring carriers to list every single employee involved in a lawful interception, the DOJ/FBI ask the Commission to "require carriers to include in their lists of designated employees only those employees who, as a regular part of their job duties, are exposed to information identifying the individuals whose communications are being intercepted pursuant to lawful electronic surveillance."²⁶ This proposal should be rejected.

The Commission already addressed this issue and agreed with those commenters who stated that requiring carriers to make a list of all designated employees was "administratively impractical."²⁷ The Commission found it sufficient to require carriers to appoint "senior authorized officer(s) or employees(s) whose job function includes being the point of contact for law enforcement to reach on a daily, around the clock basis."²⁸ The Commission further directed "carriers to include a description of the job function(s) of such points of contact and a method to enable law enforcement authorities to contact the individual(s) employed in this capacity in their policies and procedures."²⁹

The DOJ/FBI fail to demonstrate how their most recent proposal eliminates the administrative burdens associated with compiling and maintaining such a list. A list of designated employees, even a list of those "who, as a regular part of their job duties, are exposed to information"³⁰ regarding electronic surveillance, would still be administratively difficult to create and maintain without significantly increasing the benefits to law enforcement. Moreover,

²⁶ *Id.* at 5.

²⁷ *Report and Order*, ¶ 25.

²⁸ *Id.*

²⁹ *Id.*

³⁰ DOJ/FBI Petition at 5.

BellSouth's experience shows that law enforcement has not had any difficulty being able to contact the appropriate persons needed to effect a court order.

In addition, every criminal investigation involving electronic surveillance is unique. Requiring carriers to commit to a single list of employees is overly burdensome and simply unnecessary. As BellSouth stated in its earlier pleadings, it has no way of knowing in advance of any particular intercept which employees or Security Department Specialists will need to have some knowledge of an authorized electronic surveillance in order to assist law enforcement.³¹ BellSouth also objects to any rule that would require non-point-of-contact individuals to be designated.

The existing requirements are more than sufficient to minimize any security breaches. As stated above, the Commission ordered carriers to appoint senior officers or employees to serve as points of contact for law enforcement to reach on a daily, around the clock basis.³² In addition, the Commission required carriers to include in their policies and procedures a description of the job function of such points of contact as well as a method to enable law enforcement to contact the designated employee.³³ No further regulation is needed.

B. The Commission Should Deny The DOJ/FBI Request To Obtain Personal Information On Designated Employees In Order To Facilitate Background Checks.

The Commission should not require carriers to maintain records on designated employees that include personal identifying information, such as dates of birth and social security numbers.

³¹ BellSouth Comments, *Communications Assistance for Law Enforcement Act*, CC Docket No. 97-214, at 13-14 (filed Dec. 12, 1997).

³² *Report and Order*, ¶ 25.

³³ *Id.*

In their Petition, the DOJ/FBI request that the list of designated employees “include the names, dates of birth, social security numbers, and workplace telephone numbers of these designated employees”³⁴ The Commission appropriately denied this same request in its *Report and Order*,³⁵ and properly “conclude[d] that such information is invasive to carrier personnel and could even compromise a carrier’s ability to maintain a secure system by identifying the personnel charged with effectuating surveillance functions.”³⁶

The DOJ/FBI request is simply a repeat of the previously rejected proposal and should be denied. Again, the DOJ/FBI fail to demonstrate that access to such information is compelling enough to justify invading an employee’s privacy. As BellSouth demonstrated in its initial comments, there is no useful purpose served for the public or the industry in requiring carriers to disclose – as the DOJ/FBI propose – personally sensitive information, ironically in the name of protecting privacy rights.³⁷ Law enforcement should not be granted free reign to perform background checks on individuals without adherence to normal processes, including subject notification.

Moreover, the Commission should not give any weight to the DOJ/FBI assertion that the “proposed limited background checks would be scarcely more intrusive than the checks routinely conducted by landlords deciding whether to rent out an apartment.”³⁸ A background check, no matter how minimal, still reveals personal information – information that may have nothing to do

³⁴ DOJ/FBI Petition at 7.

³⁵ *Report and Order*, ¶ 25.

³⁶ *Id.*

³⁷ BellSouth Comments, *Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, at 14 (filed Dec. 12, 1997).

³⁸ DOJ/FBI Petition at 6.

with an employee's ability to perform his/her job. There are appropriate safeguards in place – especially with the addition of the Commission's systems security and integrity rules – that make the further restrictions sought by the DOJ/FBI unnecessary. For example, the criminal sanctions contained in Title 18 and BellSouth's existing internal policies serve to protect its customers' privacy and ensure appropriate assistance to law enforcement.

C. The Commission Should Reject The DOJ/FBI Request To Require Designated Employees To Sign Non-Disclosure Agreements.

The Commission should deny the DOJ/FBI proposal to require designated employees to sign non-disclosure agreements.³⁹ In its *Report and Order*, the Commission "decline[d] to adopt the FBI's recommendation[] to require carriers . . . to compel their personnel to sign nondisclosure agreements."⁴⁰ As the Commission noted, "[w]hile we do not dispute that such practices may ensure a greater level of internal carrier systems security, we believe that carriers will take necessary actions to perform their duty to ensure lawfully authorized interceptions of communications or access to call-identifying information."⁴¹ The Commission struck the appropriate balance and should not change its ruling.

BellSouth continues to oppose any rule requiring designated personnel to sign non-disclosure agreements. According to the DOJ/FBI, "[i]t remains unclear what persuasive objection could be raised to such a requirement."⁴² One persuasive objection is simply that it is not necessary because carrier safeguards are already in place to protect against the improper

³⁹ *Id.* at 7.

⁴⁰ *Report and Order*, ¶ 26.

⁴¹ *Id.*

⁴² DOJ/FBI Petition at 7.

disclosure of information pertaining to surveillance activities. Moreover, even the DOJ/FBI recognize that such a requirement is “duplicative” and involves “overlap” and “replicat[ion].”⁴³

BellSouth already addresses the importance of protecting sensitive information in its policies and procedures. Although BellSouth does not generally require its employees to sign non-disclosure agreements, employees must acknowledge company policy, which includes a non-disclosure obligation and a requirement to protect sensitive information. Prudent business practice all but dictates that carriers take reasonable steps to ensure that those employees involved in electronic surveillance activities are trustworthy. Carriers should continue to retain the authority to manage their own operations and supervise their own employees in accordance with such a corporate policy.

Another objection to the DOJ/FBI proposal is that it all but converts carriers into agents for law enforcement by imposing a duty on carriers to require their employees to sign non-disclosure agreements essentially for the benefit of law enforcement. This responsibility goes far beyond a carrier’s obligations under CALEA, which imposes a duty on telecommunications carriers to provide law enforcement with “assistance.” There is a clear distinction between providing technical assistance as required by statute versus serving as an agent of law enforcement. CALEA clearly does not require carriers to perform the latter function. Moreover, requiring carriers to act as agents for law enforcement creates a host of duties among law enforcement, carriers, and carrier personnel that could give rise to significant liability issues. To avoid the morass of legal consequences associated with an agency relationship, the Commission

⁴³ *Id.*

should reject the DOJ/FBI proposal to mandate that carriers require employees to sign non-disclosure agreements.

D. The Commission Should Affirm Its Denial Of The DOJ/FBI Request To Require Carriers To Provide A Surveillance Status Message.

In its *Report and Order*, the Commission appropriately denied the prior DOJ/FBI request to require carriers to provide law enforcement with the surveillance status message capability.⁴⁴

In denying this previous proposal, the Commission properly concluded “that a surveillance status punch list item is not an assistance capability requirement under section 103.”⁴⁵ The Commission found that the surveillance status message was not required because it was not call-identifying information as defined by CALEA.⁴⁶ Moreover, the Commission expressed its “confiden[ce] that carriers and LEAs [law enforcement agencies] will work together to ensure that a wiretap is functioning correctly.”⁴⁷

The DOJ/FBI have now developed a new argument that also must fail. Instead of asserting that the surveillance status message is mandated under section 103 as an assistance capability, the DOJ/FBI claim that this feature is required under the systems security and integrity provisions of section 105. According to the DOJ/FBI, “the surveillance status message capability falls squarely within the mandate of § 105, and should be incorporated in the

⁴⁴ *Third Report and Order*, ¶ 101. The Commission also denied the DOJ/FBI proposal to require carriers to provide two other capabilities referred to jointly by the FBI as “surveillance integrity” – (1) continuity check tone and (2) feature status message. The Commission determined that these capabilities were not required under the plain language of CALEA. *Third Report and Order*, ¶¶ 106, 111.

⁴⁵ *Third Report and Order*, ¶ 101.

⁴⁶ *Id.*

⁴⁷ *Id.*

Commission's rules implementing that provision."⁴⁸ This is nothing more than a transparent attempt to add an extra feature that the Commission correctly rejected. Accordingly, for the reasons set forth below, the Commission should deny this DOJ/FBI proposal.

First, the argument that the surveillance status capability is required under section 105 – though perhaps creative – is flawed. This capability is not mandated by section 105 – nor any other statutory provision. Section 105 of CALEA and section 229 of the Communications Act address carrier *policies and procedures* – not assistance capabilities. The assistance capability requirements are set forth in section 103, and the Commission has already ruled that the provision of the surveillance status message to law enforcement falls beyond the scope of CALEA. As the Commission explained, “the plain language of section 105 of CALEA and section 229(b) and (c) of the Communications Act reflects a Congressional concern regarding the necessity of rules to ensure that carriers have *policies and procedures* in place”⁴⁹ to govern carriers and their employees while assisting law enforcement to conduct electronic surveillance. The surveillance status message is clearly not a “policy or procedure” and is, therefore, not required by section 105. The Commission should deny this obvious attempt by the DOJ/FBI to circumvent CALEA.

Second, there are significant technical impediments to providing this feature. As BellSouth demonstrated in its initial comments, the standards organization chose not to standardize a surveillance status message because it only makes sense in certain distribution architectures (*e.g.*, when only a single switch is involved in the surveillance and the status of the

⁴⁸ DOJ/FBI Petition at 8.

⁴⁹ *Report and Order*, ¶ 17 (citing House Report at 23).

one element of the surveillance can be readily verified). For this purpose, an optional Connection Test Message was included in J-STD-025 in Annex E. For networks like cellular networks in which the surveillance is necessarily distributed, or in cases where a distribution box is used to consolidate content and call identifying information from several network elements and deliver it simultaneously to multiple law enforcement collection sites, it is impossible to verify the status of all elements and create a valid surveillance status message.⁵⁰ In light of the foregoing, the Commission should reject the DOJ/FBI proposal to require carriers to provide a surveillance status message under section 105.

E. The Commission Should Not Modify Its Rule Regarding Reporting Suspected System Security Breaches.

In its *Report and Order*, the Commission rejected the DOJ/FBI request that carriers report security compromises to the affected law enforcement agencies within two hours.⁵¹ The Commission “decline[d] to impose a specific time frame within which a carrier must report a security breach,” and “[i]nstead require[d] carriers to report such *breaches within a reasonable period of time and in compliance with any other relevant statutes*.”⁵² The DOJ/FBI now ask the Commission to modify the language of this rule to require carriers to report breaches “as soon after discovery as is reasonable in light of privacy and safety concerns and *the needs of law enforcement*.”⁵³

⁵⁰ See BellSouth Comments, *Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, at 13 (filed May 20, 1998).

⁵¹ *Report and Order*, ¶ 38.

⁵² *Id.* (emphasis added); codified at 47 C.F.R. §64.2103(e).

⁵³ DOJ/FBI Petition at 10 (emphasis added).

The Commission should deny this request and leave the rule as written. The existing rule appropriately allows carriers flexibility when reporting suspected breaches. The DOJ/FBI have not cited any evidence of problems in this area that would warrant a change in the requirement. The rule as adopted by the Commission is more than adequate to ensure that carriers report suspected breaches in a timely fashion. Accordingly, the Commission should retain its existing rule and require carriers to report breaches *within a reasonable period of time and in compliance with any other relevant statutes.*⁵⁴

CONCLUSION

The record overwhelmingly supports the Commission's conclusion that overly detailed rules are unnecessary to ensure compliance with the systems security and integrity provisions of CALEA. Existing statutory and regulatory requirements, in conjunction with current carrier policies and procedures, are more than sufficient to ensure that only lawfully authorized electronic surveillance occurs. In addition, the lack of credible evidence that these practices have


⁵⁴ *Report and Order*, ¶ 36 (emphasis added).

resulted in security breaches supports a finding that no additional rules or modifications are warranted. Accordingly, the Commission should deny the DOJ/FBI Petition.

Respectfully submitted,


BELLSOUTH CORPORATION

By:


M. Robert Sutherland
Angela N. Brown
1155 Peachtree Street, N.E.
Suite 1700
Atlanta, GA 30309-3610
(404) 249-3392


BELLSOUTH TELECOMMUNICATIONS, INC.

By:


J. Lloyd Nault, II
4300 BellSouth Center
675 West Peachtree Street, N. E.
Atlanta, GA 30375
(404) 335-0737


BELLSOUTH CELLULAR CORP.

By:


S. Kendall Butterworth
1100 Peachtree St., N.E.
Suite 910
Atlanta, GA 30309-4599
(404) 249-0919

BELLSOUTH WIRELESS DATA, L.P.


By:


Michael W. White
10 Woodbridge Center Drive, 4th Floor
Woodbridge, NJ 07095-1106
(732) 602-5453

Date: February 7, 2000

CERTIFICATE OF SERVICE

I do hereby certify that I have this 7th day of February, 2000, served the following parties to this action with a copy of the foregoing **BELLSOUTH OPPOSITION**, reference CC Docket No. 97-213, by hand delivery or by placing a true and correct copy of the same in the United States Mail, postage prepaid, addressed to the parties on the attached service list.



Lenora Biera-Lewis

SERVICE LIST
CC DOCKET NO. 97-213

Magalie Roman Salas, Commission Secretary*
Portals II
445 12th Street, SW
Suite TW-A235
Washington, DC 20554

International Transcription Service*
1231 20th Street, NW
Washington, DC 20554

Larry R. Parkinson
General Counsel
Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Washington, DC 20535

Douglas N. Letter
Deputy Associate Attorney General
US Department of Justice
Room 5241
950 Pennsylvania Avenue, NW
Washington, DC 20530

L. Marie Guillory
Jill Canfield
4121 Wilson Boulevard
10th Floor
Arlington, VA 22203

* BY HAND DELIVERY

Attorneys for National Telephone Cooperative Association